

Security Awareness Newsletter

May 2003

Spam On the Increase	Going Wireless?	Cyber Bytes
Security Incident Reporting	Password Audits	Microsoft Information
Spyware	Security Badge FAQs	Useful URLs

Foreword

In an effort to emphasize the importance of IT security issues to all staff and to promote security awareness, the GOT Division of Security Services is pleased to provide the Security Awareness Newsletters. We hope these newsletters will be a valuable resource, providing practical tips, security solutions, and job-saving techniques.

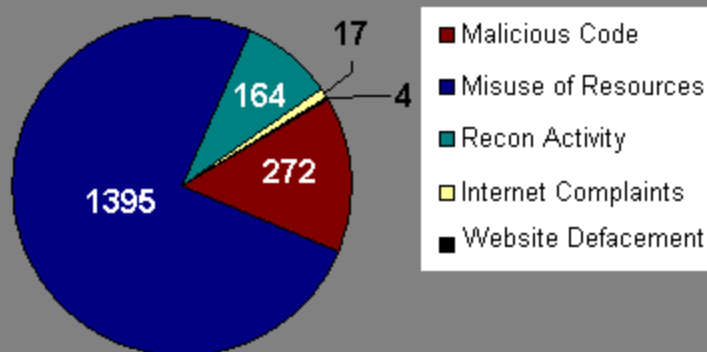
Also, as a friendly reminder, GOT staff are encouraged to familiarize themselves with all security policies, manuals, and procedures which can be found at <http://www.gotsource.net/dscgi/ds.py/View/Collection-485>.

Spam on the Increase

The number of Spam incidents reported to GOT in April grew to nearly 900, more than the number reported during the prior 7 months combined. While GOT realizes that this increase can be attributed to a growing Spam trend, it is also believed that improved security incident reporting by agencies may also be a factor. GOT would like to encourage everyone to continue reporting all security incidents to the Division of Security Services. Increased incident reporting is especially crucial since it provides a means for GOT to measure the volume of Spam and use this information as a tool in acquiring funding for solutions to reduce or alleviate the problem. The following article contains additional information on reporting security incidents to GOT.

GOT has developed procedures and a guide which may help you reduce or eliminate your exposure to these unwanted emails. The information can be found at http://www.state.ky.us/got/ois/security/faqs_Unsolicited%20email.htm.

GOT Security Incident Report Statistics January thru April 2003



Key Definitions:

Malicious Code includes activity involving viruses, worms, Trojans, etc.

Misuse of Resources includes inappropriate use of email or other state resources (Spam, chain letters, etc.), illegal login attempts, storage and distribution of illegal software, hoaxes, etc.

Reconnaissance Activity includes network probes and scans, as well as unauthorized monitoring.

Internet Complaints are usually complaints from outside

the Commonwealth's network involving Spam, chain letters, network probes/scans, etc., that involve a network device within the Commonwealth's domain.

Website Defacement is the compromise of a web server by an intruder, usually involving the altering or defacing of data on the web page.

GOT Wants YOU to Report Security Incidents!



Since January 2003, the Governor's Office for Technology has investigated over 1,800 computer-related security incidents. These incidents range from events such as Spam and chain letters to website defacements to the reporting of malicious code activity (viruses, worms, Trojans). These incidents occur every day and even though some may not pose an immediate threat, it is important that all security-related incidents be reported immediately to GOT's Division of Security Services (DSS). GOT relies on the vigilance of its staff and customers to report these incidents so that they can be investigated and remediated, safeguarding the Commonwealth's computing resources.

What is a security incident? A security incident can be defined as any adverse event threatening computer security. The adverse event may potentially lead to loss of data confidentiality, compromised data or system integrity, or decreased availability and/or denial of access to an information system and/or network.

Incidents generally fall into two categories: physical and electronic. Physical security incidents include, but are not limited to, breaches of physical security policies such as unauthorized access to a facility; theft or damage to computer equipment or media; bomb threats; or natural

disasters such as a fire, flood, or tornado.

Electronic security incidents include any suspicious activity (malicious or benign) that may jeopardize the security of the KIH networks, servers, workstations, or other computing resources or that violates enterprise policies. Examples include, but are not limited to, unauthorized computer access; inappropriate computer use (surfing pornographic websites, using Commonwealth computer resources for non-business related activity, etc.); cyber attacks; website defacements; sending or forwarding spam, pornographic email, or chain letters; or exposure to computer viruses or other malicious code.

How do I report a security Incident? If you encounter an incident that you feel is suspicious, report it immediately to DSS by completing a [Security Incident Reporting Form \(GOT-012\)](#) and forwarding via email to [GOT Security Services ISS](#). Only through diligence and cooperation can the Commonwealth protect and preserve the integrity of its computing environment.

The Security Incident Reporting Form can be found at the following webpage:
www.gotsource.net/dscgi/ds.py/Get/File-1921/Security_form_GOT_F012_Form.doc

I Spy Spyware

What is Spyware? According to Whatis.com, the definition of Spyware is "any technology that aids in gathering information about a person or organization without their knowledge." Other names for Spyware include Adware (although not all Adware is considered Spyware), Foistware, and Hijackware.



Spyware can include hardware devices such as keyloggers that are secretly placed on the cable between the keyboard and the computer to record keystrokes, or it can be programming code that is concealed in software or cookies and covertly collects user data. Users often unknowingly download Spyware in seemingly innocent freeware/shareware products such as peer-to-peer file sharing programs. Spyware can also be distributed like viruses with users opening apparently benign executable files and unleashing the code.

What is the Purpose/Capability of Spyware? Spyware's main purpose is to gather data about the user (usually web surfing habits) and forward it to advertisers or other interested parties. Some additional functions of Spyware may include keystroke monitoring, scanning files on the hard drive, snooping applications such as chat programs, installing other Spyware programs, reading cookies, and changing the default home page of a web browser.

Spyware is most often veiled as an independent executable file embedded with many freeware and shareware products available via the Internet. Developers often partner with advertisers to include Spyware in their products in order to recoup some of the expense for software development.

Is Spyware Legal? While Spyware is not considered illegal, certain privacy and ethics issues are involved that make many people uneasy. The covert collection of data and statistics without the user's knowledge or permission and the hidden use of the Internet connection to relay this information back to the advertiser or other interested groups are generally considered unwelcome features. In addition, there is always the possibility of Spyware collecting password or credit card information. Many legitimate companies notify users of the Spyware by including statements in their software license agreements. Unfortunately, users often overlook these notifications. It should also be noted that simply uninstalling the freeware may not remove the Spyware that came bundled with the product since it remains buried in the Windows' registry. A listing of software products that contain Spyware can be found at the following website:

http://pestpatrol.com/Support/About/About_Products_Incorporating_Spyware.asp.

It should be noted that installing unapproved freeware or shareware onto GOT computers is not permitted according to GOT policy. Any exception to this policy must be documented on a [Security Exemption Request \(GOT-F085\)](#) and submitted to the Director of Security Services. The Security Exemption Request can be found at the following webpage:

www.gotsource.net/dscgi/ds.py/Get/File-13130/SS_GOT-F085_security_exemption_req_.dc

How Can I get Rid of Spyware? Currently, the Commonwealth does not have an approved Enterprise product to detect and remove Spyware; however, the following software have been recommended by PC Magazine as being the top Spyware removal products. It should be noted that none of the software below should be considered a complete solution for thoroughly protecting systems. It is recommended that a combination of anti-virus, anti-trojan, anti-spyware and personal firewall software (such as BlackICE or ZoneAlarm) be used to provide comprehensive protection from malicious code, intruders, etc. As always, consult with your network administrator before installing any of these products.

PepiMKSpybot Search & Destroy - <http://security.kolla.de/>

Lavasoft Ad-aware 6 - <http://www.lavasoft.de/software/adawareprofessional/>

Aluria's Spyware Eliminator - <http://www.aluriasoftware.com/spywareeliminator/>

BPS Spyware/Adware Remover - <http://www.bulletproofsoft.com/index.html>

Spy Remover 5.0 - <http://www.rizalsoftware.com/>

Internet Cleanup 3.0 - <http://www.aladdinsys.com/internetcleanup/>

PestControl - <http://pestpatrol.com/pestpatrolhe/>

Additional reading on the subject can be found in the following white paper: Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security - <http://www.pestpatrol.com/Whitepapers/CorporateSecurity0403.asp>

Thinking about Going Wireless?



Wireless LANs are a wonderful thing! No wires to tie you down... access to the world at your fingertips just about anywhere, anyplace. Who could ask for more? Well, you might want to think again. The new wireless LAN (WiFi) technology that everyone is raving about has some serious security risks that could compromise confidential information and provide a back door for intruders to traditional wired networks. In fact, the risks are so substantial that the Commonwealth's CIO, Aldona Valicenti, has required that all

proposed wireless network implementations that will provide access to the Kentucky Information Highway (KIH) be reviewed and approved by GOT before deployment

GOT is currently working on an enterprise policy for wireless LAN technology. A few of the proposed requirements are listed below:

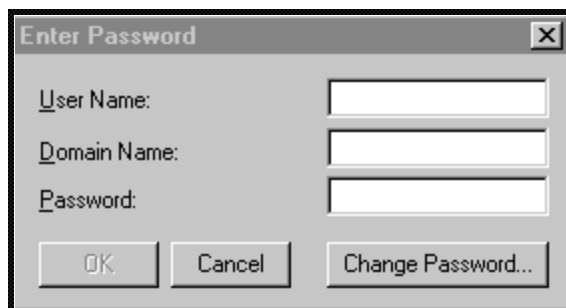
- Due to multiple security flaws in WEP (wireless' built-in security) a wireless LAN must be supplemented with a virtual private network (VPN) solution. VPN clients should be installed on all attached devices.
- Firewalls must be installed between wireless and traditional LANs and must implement a block all, allow few rule set. In addition, all wireless LAN clients must have personal firewall software installed.
- All Access Point (AP) configuration parameters (SSID, keys, passwords, channels, etc) that can be changed from the default manufacturer settings must be changed from the default.
- Sensitive/confidential data must not be transmitted via wireless LANs unless strong cryptography is used.
- All security measures implemented for traditional LANs, including adequate encryption and authentication mechanisms, must also be utilized for wireless LAN installations.

For more information on the security implications of wireless LANs, check out the National Institute of Standards & Technology's wireless network security white paper: Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, which can be found at the following webpage : http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

ComputerWorld.com also has a good article on monitoring wireless networks that is recommended reading which can be found at <http://www.computerworld.com/securitytopics/security/story/0,10801,80742,00.html>

Password Audits

If you've been asked to change your password recently, chances are you were one of many who have had their passwords cracked by the Division of Security Services (DSS). GOT is performing password audits in an effort to ensure that GOT staff are complying with the [Enterprise UserID and Password Policy \(CIO-072\)](#). Every quarter, DSS will receive a listing of staff passwords and use a password cracking software to identify weak, non-compliant passwords. Those staff whose passwords are cracked will be required to create a new policy-compliant password. Keep in mind that passwords must be:



Windows Users:

- Eight (8) characters or more (11 if the UserID has privilege rights, network administrator, etc.).
- Upper **and** lower case letters.
- Contain at least 1 number.
- Contain at least 1 special character.
- Must not contain a name, word in a dictionary, or phrase.

Mainframe Users:

- Exactly eight (8) characters - no more, no less.
- Contain at least 1 number.
- Contain at least 1 special character (mainframe will only allow the use of @, #, or \$).
- Must not contain a name, word in a dictionary, or phrase.

Security Badge FAQs



You're probably well aware of the GOT policy that requires all GOT employees, contractors, vendors, etc. to have a security badge. And you probably also know that you need to wear your badge at all times and display it prominently. But do you know what to do if your badge is lost or which form to fill out to request additional access to other GOT buildings or floors at the Commonwealth Data Center? The following provides some answers to frequently asked questions regarding security badges:

What should I do if I lose or misplace my badge? Report it immediately to the [Division of Security Services \(DSS\)](#). DSS staff will deactivate the badge and issue you a temporary badge with access to your workstation floor/building. If you are unable to locate the badge after 24 hours, a new badge will be issued to you.

My badge is damaged. What can I do to get a new one? Contact [DSS](#) to issue you a new badge. At this time, there is no charge for replacing a damaged badge.

I left my badge at home. What should I do? Contact [DSS](#) to issue you a temporary badge that will give you access to your workstation floor/building.

I work at the CDC but need access to Fair Oaks to work on a project that I've been assigned to for the next few months. How do I request additional badge access?

Have your branch manager or director complete a [Request for Security Badge Access \(GOT-F019\)](#) and submit it to [DSS](#). Be sure to indicate on the form both current and additional access required. Also note that a change in building access for vendors or other state personnel requires approval by the appropriate division director and/or executive director.

I have a new employee, what do I need to do to get him/her a new badge? The new employee's branch manager should complete a Request for Security Badge Access (GOT-F019). The signed form needs to be brought with the employee to the photograph session. The employee's photo will be taken at the CDC building (101 Cold Harbor Drive). You can contact Cathy Hall via [email](#) or phone (564-8782) to arrange an appointment time. Vendors or other state agency staff that need a badge, will need to have the appropriate GOT director or executive director also sign the GOT-F019.

An employee in my branch has recently been terminated, what should I do? The employee's immediate supervisor should reclaim the badge and contact DSS immediately to deactivate the employee's building access.

I'm a GOT customer and have servers housed at the Commonwealth Data Center that I need to access. How do I obtain entry to the CDC? The same process should be followed as that of a GOT employee, except that the appropriate GOT division director/executive director must sign the Request for Security Badge Access (GOT-F019). The signed form needs to be brought with the customer to the photograph session at the CDC building (101 Cold Harbor Drive). You can contact Cathy Hall via [email](#) or phone (564-8782) to arrange an appointment time.

Additional Important Security Badge Information

- Badges must not be loaned to other people.
- Badges must not be misused or modified in any way.
- Badges must be displayed at all times.
- Do not allow anyone to "piggyback" into a building on your badge.
- Vendors or other state agency personnel do not have authority to sign in visitors that have not been issued a GOT security badge.

To find out more information on Security Badges and other security-related subjects, check out the Division of Security Services FAQ webpage at <http://got.ky.gov/NewsItem.aspx?TYPE=FAQ&WHICH=20>.

The Request for Security Badge Access (GOT-F019) can be found at the following webpage:
http://www.gotsource.net/dscgi/ds.py/Get/File-2842/GOT_F019REV2.rtf

Cyber Bytes



Spam: Not Just for Your Computer Anymore

According to recent article on Wired News.com, your cell phone is the next target for spammers. Text messaging, an option on newer cell phones, provides a new mode for the distribution of unwanted and unsolicited junk mail. For more information, check out this article at <http://www.wired.com/news/technology/0,1282,58704,00.html>.

New Hampshire May Legalize War Driving

A bill has been introduced to the New Hampshire legislature that will legalize war driving in that state. The bill states that owners of wireless LANs must secure them or lose some of their rights to prosecute intruders. For more information, check out this article at <http://www.wired.com/news/wireless/0,1382,58651,00.html>.

No Support for Federal Spam Legislation

Attorney Generals from 44 states and the District of Columbia have indicated they will not support current legislation in Congress to cut down on Spam. For more information, check out this article at <http://www.securityfocus.com/news/4378>.

How to Ensure Security Compliance with HIPAA

The HIPAA privacy rule took effect April 14. To find out how this may affect you, access the following website:
<http://www.computerworld.com/securitytopics/security/story/0,10801,80812,00.html>

[Back to Top](#)

Microsoft Information

Security Update for Microsoft Internet Explorer

A number of security issues have been identified in Microsoft Internet Explorer that could allow an attacker to compromise your Microsoft Windows-based systems. For more information on this vulnerability and where to download patches, access the following link
<http://www.computerworld.com/securitytopics/security/story/0,10801,80812,00.html>.

Security Update for Microsoft Windows

A security issue has been identified that could allow an attacker to compromise a computer running Microsoft Windows and gain control over it. For more information on this issue and where to download patches, access the following link

http://www.microsoft.com/security/security_bulletins/ms03-013.asp.

Security Update for Microsoft Proxy Server 2.0 and Microsoft Internet Security and Acceleration (ISA) Server 2000

A security issue has been identified that could allow an attacker to cause a computer running Microsoft Proxy Server 2.0 or Microsoft Internet Security and Acceleration (ISA) Server 2000 to stop responding to Internet requests. This issue only affects computers acting as servers. For more information on this issue and where to download patches, access the following link http://www.microsoft.com/security/security_bulletins/ms03-012.asp

[Back to Top](#)

Useful URLs

www.cert.org

The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

www.nai.com

Network Associates aspires to be the worldwide leader in network security and availability for e-business. Founded as McAfee Associates in 1989, Network Associates, Inc. was created by the merger of McAfee Associates and Network General in December of 1997.

www.securityfocus.com

Security Focus ensures the integrity of enterprises' assets through its SIA – Security Intelligence service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through email, voice message, fax, or SMS (Small Message Service) on wireless phones. SIA provides all known information available about vulnerabilities, their causes, and severities creating actionable information to bolster computers from attack.

<http://www.zdnet.com/>

ZDNet operates a worldwide network of websites for people who want to buy, use, and learn about technology. Winner of the Computer Press Association's "Best Overall Site" award for two consecutive years, ZDNet provides an invaluable perspective and resources for technology decision makers to gain an edge in business.

<http://www.searchsecurity.com/>

SearchSecurity.com is the home of TechTarget, offering the most targeted media for enterprise IT professionals, including industry-specific websites, more than 100 email newsletter titles, print media, exclusive, invitation-only conferences, live online events and list rentals.

[Back to Top](#)

Sources: Wired.com, Microsoft.com, PestPatrol.com, NIST, CNN, SecurityFocus.com, ComputerWorld.com, Whatis.com